IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Inventors: Amit Bagga et al.

Serial No.: 10/723416

Conf. No.: 2635

Filing Date: 11-26-2003

Art Unit: 2435

Examiner: Patel, Nirav B

Docket No.: 633-038US

Title: Method and apparatus for extracting authentication information from a user

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

APPEAL BRIEF UNDER 37 CFR 41.67

Pursuant to 37 CFR 41.67, this brief is filed in support of the appeal in this application.

TABLE OF CONTENTS

REAL PARTY IN INTEREST

The real party of interest in this application is the assignee of this application: Avaya, Inc. of Baskin Ridge, New Jersey.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

STATUS OF CLAIMS

Claims 1, 2, 4-14, and 16-25 stand rejected and are being appealed.

Claims 3 and 15 have been canceled.

STATUS OF AMENDMENTS

All amendments have been entered.

SUMMARY OF THE CLAIMED SUBJECT MATTER

Authentication is the process of determining whether a person is, in fact, who the person declares to be. On the Internet, authentication is commonly accomplished through the use of a password. Knowledge of the password is assumed to guarantee that the identity of the submitter of the password is authentic.

In order for the password to be a reliable means for authentication, the password must be sufficiently strong. At the same time, it is also desirable that the password be easy to remember by the user. In other words, a good password is easy for a user to remember, and yet not easily guessed by an attacker.

In query directed authentication, a user is asked personal questions, such as the user's social security number, date of birth or mother's maiden name. The query can be thought of as a ***hint*** to "pull" a fact from a user's long term memory. As such, the answer need not be memorized. ***See* the Specification at paragraph [0004]**

Stated succinctly, in query directed authentication, *the personal information of a user can be utilized as a password.*

Passwords that are based on personal information satisfy the requirement to be easily remembered. However, many of these passwords are also easily guessed by an attacker.

For example, the birth date of a person is often published on the user's social networking web sites, such as Facebook and Myspace. When the birth date of a user is used as a password, a potential attacker can obtain it by simply performing a search on the Internet. Therefore, birth dates are not suitable for use as passwords for people with social networking web pages.

In contrast, the maiden name of a user's mother is likely suitable for a password. Maiden names rarely come up in conversation, so third parties are unlikely to know the maiden name of a user's mother. By the same token, maiden names are usually not published on social networking web sites. Therefore, maiden names, on average, constitute stronger passwords than birth dates.

The present invention is a method and apparatus for determining which items of personal information are suitable for use as passwords and which are not.

In accordance with the invention, a user is requested to choose from a set of topics from which personal information is to be drawn. The topic may include the user's personal history, the user's personal preferences, *etc.* ***See* the Specification at paragraph [0032]**

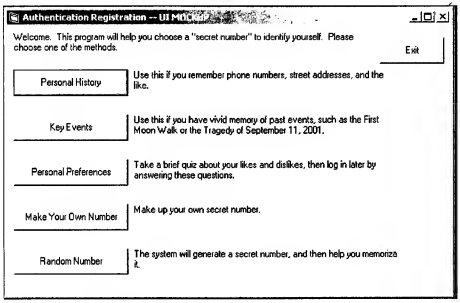

Figure 6 of the Application: An exemplary user interface for selecting a topic.

After a topic is selected, the user is asked to provide personal information associated with the selected topic. The personal information provided, will become the user's password if it is determined to be suitable by the present invention. ***See* the Specification at paragraph [0032]**

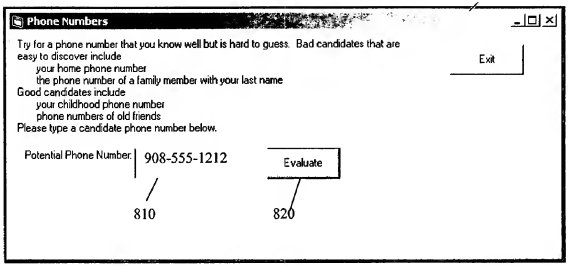

Figure 8 of the Application. An exemplary user interface that allows the user to enter a proposed answer.

For example, if the user selects the "Personal History" topic, the user is asked to provide a telephone number that is familiar to the user. The telephone can be the user's childhood telephone number (*i.e.* "732-555-1212") or the phone number of a person that is important to the user. ***See* the Specification at paragraph [0007]**

Additionally, the user is asked to select a hint, or reminder, associated with the provided personal information. ***See* the Specification at paragraphs [0007] and [0032]**

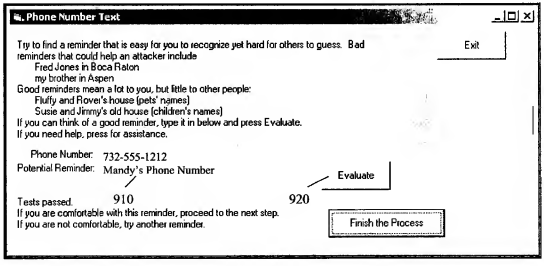

Figure 9 of the Application: An exemplary interface that allows the user to enter a proposed hint.

As discussed above, the hint is a question, or a challenge, that provokes the user to enter an item of personal information which the user elected to use as a password. At a later time, when the user is asked to enter his or her authentication information, the user will be presented with one or more hints in response to which the user has to provide corresponding personal information.

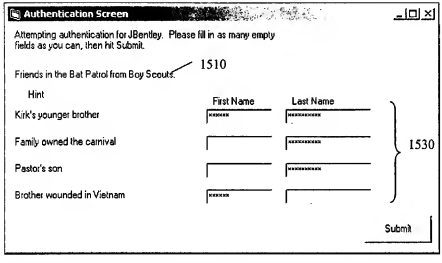

Figure 15 of the Application: An exemplary user interface that may be employed by the verification process to obtain user answers in response to a challenge

After the personal information and/or the hint are selected, ***a test is performed by the present invention to determine if both the answers or reminders (or both) are correlated with the user***. The purpose of the test is to ensure that the personal information which the user is going to use as a password is not easily obtained by an attacker. ***See* the Specification at paragraph [0033]**

In the present invention, one or more rules may be defined to ensure that a given item of personal information is not correlated with the user. "For example, if a user selects a telephone number of a person, the information extraction analysis can determine if there is a predefined relationship between the owner of the telephone number and the user, such as a family member (self, sibling or parent). *The analysis correlates the number to the person by analyzing the number of hits obtained by using a search engine such as*

Google.com where both the person and number appear on the same page. If the number of hits is higher than a chosen threshold, then a positive correlation is said to exist. ***See* the Specification at paragraph [0033]**

If it is determined that the answer can be correlated to the user, the answer is discarded and the user is prompted to provide new personal information. If the answer cannot be correlated to the user, the answer is stored in a database record. ***See* the Specification at paragraph [0035]**

For example, if the user chose to use the telephone number 732-555-1212 and the name of the user is John Smith, an Internet search will be performed in which the search string is "John Smith 732-555-1212." ***See* the Specification at paragraph [0033]**

After the Internet search is performed, the present invention will count the number of web pages found that contain references to both the name John Smith, and the phone number. ***If the number of web pages found exceeds a certain predefined threshold, the telephone number is deemed not suitable for use as a password****. So, the telephone number is rejected and the user is asked to provide another item of personal information.* ***See* the Specification at paragraph [0033]**

The present invention comprises three (3) independent claims. Each shall be presented, summarized, and mapped to the specification and the drawings, if any.

Independent claim 1 recites:

> 1. A method for generating a password for a user during an enrollment phase, comprising:
>
> presenting said user with a plurality of topics;
>
> receiving a user selection of at least one topic;
>
> receiving one or more personal details from said user associated with said at least one selected topic as a proposed password;
>
> performing an Internet search using a query containing one or more keywords derived from said personal details of said proposed password, wherein said Internet search searches contents of the Internet across a plurality of web sites using a search engine tool;
>
> evaluating results of said search relative to one or more predefined thresholds applicable to said at least one selected topic;
>
> rejecting said proposed password when said user is correlated with said proposed password if one or more of said predefined thresholds are exceeded by said results; and
>
> recording said one or more personal details as a password for said user if said proposed password is not rejected.

Claim 1 is described in Figures 4-15 of the Specification and in paragraphs [0032]-[0055].

Independent claim 13 recites

> 13. An apparatus for generating a password for a user during an enrollment phase, comprising:
>
> a memory; and
>
> at least one processor, coupled to the memory, operative to:
>
> present said user with a plurality of topics;
>
> receive a user selection of at least one topic;
>
> receive one or more personal details from said user associated with said at least one topic as a proposed password;
>
> perform an Internet search using a query containing one or more keywords derived from said personal details of said proposed password, wherein said Internet search searches contents of the Internet across a plurality of web sites using a search engine tool;
>
> evaluate results of said search relative to one or more predefined thresholds applicable to said at least one selected topic;
>
> reject said proposed password when said user is correlated with said proposed password if one or more of said predefined thresholds are exceeded by said results; and
>
> recording said one or more personal details as a password for said user if said proposed password is not rejected.

Claim 13 is described in Figures 4-15 of the Specification and in paragraphs [0032]-[0055].

Independent claim 25 recites:

> 25. An article of manufacture for generating a password for a user during an enrollment phase, comprising a machine readable storage medium containing one or more programs which when executed implement the steps of:
>
> presenting said user with a plurality of topics;
>
> receiving a user selection of at least one topic;
>
> receiving one or more personal details from said user associated with said at least one selected topic as a proposed password;
>
> performing an Internet search using a query containing one or more keywords derived from said personal details of said proposed password, wherein said Internet search searches contents of the Internet across a plurality of web sites using a search engine tool;
>
> evaluating results of said search relative to one or more predefined thresholds applicable to said at least one selected topic;
>
> rejecting said proposed password when said user is correlated with said proposed password if one or more of said predefined thresholds are exceeded by said results; and
>
> recording said one or more personal details as a password for said user if said proposed password is not rejected.

Claim 25 is described in Figures 4-15 of the Specification and in paragraphs [0032]-[0055].

GROUNDS OF OBJECTION AND REJECTION TO BE REVIEWED ON APPEAL

Ground 1: Double Patenting Rejection of Claims 1, 2, 4-14, and 16-25

Claims 1, 2, 4-14, and 16-25 were provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-27 of co-pending application No. 10/815191 in view of co-pending Application No. 10/674288.

Ground 2: 35 U.S.C. 103 Rejection of Claims 1, 8, 13, 20, and 25

Claims 1, 8, 13, 20, and 25 were rejected under 35 U.S.C. 103 as being unpatentable over six (6) references:

1. M. Nelson, U.S. Patent 7,062,655 (hereinafter "Nelson") in view of
2. E. Ogura, U.S. Publication 2004/0078603 (hereinafter "Ogura") in view of
3. D. Fallman, U.S. Publication 2004/0107406 (hereinafter "Fallman") in view of
4. R. Eitel, U.S. Patent 7,043,521 (hereinafter "Eitel") in view of
5. A. Mikheev, U.S. Publication 2002/0055919 (hereinafter "Mikheev") in view of
6. J. Lee, U.S. Publication 2004/0044657 (hereinafter "Lee").

Ground 3: 35 U.S.C. 103 Rejection of Claims 2, 7, 11, 14, 19, and 23

Claims 2, 7, 11, 14, 19, and 23 were rejected under 35 U.S.C. 103 as being unpatentable over fseven (7) references:

1. M. Nelson, U.S. Patent 7,062,655 (hereinafter "Nelson") in view of
2. E. Ogura, U.S. Publication 2004/0078603 (hereinafter "Ogura") in view of
3. D. Fallman, U.S. Publication 2004/0107406 (hereinafter "Fallman") in view of
4. R. Eitel, U.S. Patent 7,043,521 (hereinafter "Eitel") in view of
5. A. Mikheev, U.S. Publication 2002/0055919 (hereinafter "Mikheev") in view of
6. J. Lee, U.S. Publication 2004/0044657 (hereinafter "Lee") in view of
7. L. Honarvar, U.S. Patent 7,231,657 (hereinafter "Honarvar").

Ground 4: 35 U.S.C. 103 Rejection of Claims 4-6, 16-18

Claims 4-6 and 16-18 were rejected under 35 U.S.C. 103 as being unpatentable over seven (7) references:

1. M. Nelson, U.S. Patent 7,062,655 (hereinafter "Nelson") in view of
2. E. Ogura, U.S. Publication 2004/0078603 (hereinafter "Ogura") in view of

3. D. Fallman, U.S. Publication 2004/0107406 (hereinafter "Fallman") in view of
4. R. Eitel, U.S. Patent 7,043,521 (hereinafter "Eitel") in view of
5. A. Mikheev, U.S. Publication 2002/0055919 (hereinafter "Mikheev") in view of
6. J. Lee, U.S. Publication 2004/0044657 (hereinafter "Lee") in view of
7. P-Synch Installation and Configuration Guide (hereinafter "P-Synch").

Ground 5: 35 U.S.C. 103 Rejection of Claims 9, 10, 12, 21, 22, and 24

Claims 9, 10, 12, 21, 22, and 24 were rejected under 35 U.S.C. 103 as being unpatentable over seven (7) references:

8. M. Nelson, U.S. Patent 7,062,655 (hereinafter "Nelson") in view of
9. E. Ogura, U.S. Publication 2004/0078603 (hereinafter "Ogura") in view of
10. D. Fallman, U.S. Publication 2004/0107406 (hereinafter "Fallman") in view of
11. R. Eitel, U.S. Patent 7,043,521 (hereinafter "Eitel") in view of
12. A. Mikheev, U.S. Publication 2002/0055919 (hereinafter "Mikheev") in view of
13. J. Lee, U.S. Publication 2004/0044657 (hereinafter "Lee") in view of
14. D. Kanevsky, U.S. Patent 5,774,525 (hereinafter "Kanevsky").

ARGUMENTS

Ground 1: Double Patenting Rejection of Claims 1, 2, 4-14, and 16-25.

Claims 1, 2, 4-14, and 16-25 were provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-27 of co-pending application No. 10/815191 in view of co-pending Application No. 10/674288.

A terminal disclaimer has been filed on March 10, 2009 along with the notice of appeal, and, therefore, the applicants respectfully submit that the rejection is overcome.

Ground 2: 35 U.S.C. 103 Rejection of Claims 1, 8, 13, 20, and 25

Claims 1, 8, 13, 20, and 25 were rejected under 35 U.S.C. 103 as being unpatentable over M. Nelson, U.S. Patent 7,062,655 (hereinafter "Nelson") in view of E. Ogura, U.S. Publication 2004/0078603 (hereinafter "Ogura") and further in view of D. Fallman, U.S. Publication 2004/0107406 (hereinafter "Fallman") and further in view of R. Eitel, U.S. Patent 7,043,521 (hereinafter "Eitel").

Claim 1 recites:

> 1. A method for generating a password for a user during an enrollment phase, comprising:
>
> presenting said user with a plurality of topics;
>
> **receiving a user selection of at least one topic;**
>
> **receiving one or more personal details from said user associated with said at least one selected topic as proposed password;**
>
> performing an Internet search using a query containing one or more keywords derived from said personal details of said proposed password, wherein said Internet search searches contents of the Internet across a plurality of web sites using a search engine tool;
>
> evaluating results of said search relative to one or more predefined thresholds applicable to said at least one selected topic;
>
> **rejecting said proposed password when said user is correlated with said proposed password** if one or more of said predefined thresholds are exceeded by said results; and
>
> recording said one or more personal details as a password for said user if said proposed password is not rejected.
>
> **(emphasis added)**

Neither Nelson, Ogura, Fallman, Lee, Mikheev nor Eitel teach or suggest, alone or in combination, what claim 1 recites — namely:

(1) The receiving a user selection of a topic, and, then, receiving one or more ***personal details associated with the selected topic,***

(2) Performing an Internet search ***using a query containing one or more keywords derived from said personal details***, *and*

(3) Performing an Internet search **in order to correlate a user with a proposed password.**

The prior art cited by the Office fails to teach an arrangement in which *personal details with a selected topic are received*. In rejecting claim 1 the Office wrote:

> Ogura teaches:
>
> Presenting said user with a plurality of topics; [Fig. 5, step 520-525]; *receiving one or more personal details from said user associated with said at least one said topic*, as a proposed password (input from user**)** [Fig. 5, steps 550-555, Fig 9, step 930].
>
> Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Ogura with Nelson to Present various topics and receiving an input from the user based on selection of the topics, since one would have been motivated to allow the authentication of the identity of the user through the user of a primary and/or secondary authentication system [Ogura, paragraph 0006].
>
> *(emphasis supplied)*
>
> ***See* the Office Action Dated 11/28/2008 on page 3**

The applicants disagree. Ogura teaches the use of answers to questions in authenticating a user. Claim 1 teaches:

(1) the selection of a topic by a user;

(2) the receiving of personal details associated with the topic; and

(3) evaluating which details are suitable are the personal details to be used as a password.

In contrast, Ogura teaches the selection of question sets, providing answers to the question sets, and using the question sets as secondary authentication. ***See the discussion of Figure 5 at* paragraphs [0044] – [0054] of Ogura** *However, Ogura does not teach evaluating the answers to determine how suitable they are to be used as passwords.*

Furthermore, claim 1 specifically recites the receiving of *personal details*. In contrast Ogura teaches the receiving of answers, *but it does not teach that the answers are in fact personal details* Therefore Ogura fails to teach what the Office suggests that it does, namely — presenting the user with a plurality of topics and receiving one or ***more personal details from said user as a proposed password***.

Furthermore, the prior art cited by the Office fails to teach an arrangement in which an *Internet search is performed to correlate a user with a proposed password.*

In rejecting claim 1, the Office wrote:

> *Further, Nelson teaches searching database using keywords based on the proposed password and verifying the proposed password as shown in Fig. 3.* Ogura teaches calculating the score/rate and comparing the score/rate with the threshold. [Fig. 9]
>
> ***See* the Office Action dated 11/28/2008 at pages 3 and 4**
>
> *(Emphasis Supplied)*

The invention of Nelson is for a method and system for determining trivial keyboard sequences of proposed passwords.

Figure 3 of Nelson, to which the Office refers, depicts a flowchart of a process for determining trivial keyboard sequences of proposed passwords using a password verification mechanism. "The password verification mechanism executes an algorithm on a proposed password utilizing one or more of three formulas designed to minimize the occurrence and assignment of trivial keyboard passwords. *The first two formulas verify that the key strokes associated with the proposed password are not on the same row and column, and the third formula assures a diverse key stroke pattern.*" ***See* Nelson, col. 5, ll. 8-15.** Therefore, Nelson does not teach what claim 1 recites — namely, verifying a proposed password, which contains personal details of a user, by performing an Internet search in order to ***correlate the password with the user.***

And still furthermore, the prior art cited by the Office does not teach an arrangement ***in which an Internet search is performed by using a query containing one or more keywords derived from a user's personal details***

In rejecting claim 1, the Office further wrote:

> *Fallman teaches: performing an Internet search using a query containing one or more keywords derived from the input entered by the user* (said details of said proposed password as disclosed by Ogura and Nelson), wherein said Internet search searches contents of the internet across plurality of web sites using a search engine tool [Fig. 1, paragraph 0073, 0074, well-known search engine/technique, please refer ***US 2002/0055919*** — Google, Alta-Vista – Fig. 1, ***US 2004/0044657*** – Yahoo – paragraph 0007]
>
> Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Fallman, with Nelson and Ogura to utilize an Internet search of the keywords entered by the user, since one would have been motivated to check the string/keyword against the Internet database to cover all occurring words that allow evaluation of the keyword/string [Fallman, paragraph 0007-0015].
>
> Fallman teaches performing the Internet search for the keywords entered by the user and evaluating the result of the search [paragraph 0014, 0015]. Fallman doesn't expressively mention based on the predefined threshold.
>
> Eitel teaches: evaluating results of said search relative to one or more predefined thresholds applicable to said at least one selected topic (input); rejecting said result if one or more said predefined thresholds are exceeded by said results [Fig. 3, col. 6 lines 46-60].
>
> Therefore it would have been obvious to one of ordinary skill in the art to combine Eitel with Nelson, Ogura, and Fallman to evaluate the search result based on the threshold, since one would have been motivated to elicit better/closer result from evaluation [Eitel, col. 5 lines 60-67].
>
> Fallman teaches: performing an Internet search using a query containing one or more keywords derived from input entered by the user (said details of said proposed password as disclosed by Ogura and Nelson), wherein said Internet search searches plurality of web sited using a search engine tool
>
> ***See* the Office Action dated 11/28/2008 at pages 3 and 4**
>
> *(Emphasis Supplied)*

The Office cites Fallman for teaching "performing an Internet search using a query containing one or more keywords derived from the input entered by the user." However, claim 1 recites, *using a query containing one or more keywords derived from said* ***personal details*** *and using the search results to* ***correlate the user with a password.*** Fallman concerns the use of the Internet for the performance of text verification, ***such as spell checking***, for various word processing programs. Fallman, does not teach: **(1)** the search

of one or more keywords derived from a user's personal details; and **(2)** the user of the search results to correlate the user with the personal details (a.k.a. the proposed password).

For these reasons, the applicants respectfully traverse the rejection of claim 1.

Because claim 8 depends on claim 1 the applicants respectfully traverse the rejection of claim 8.

Independent claim 13 recites:

> **13.** (Previously Presented) An apparatus for generating a password for a user during an enrolment phase, comprising:
>
> a memory; and
>
> at least one processor, coupled to the memory, operative to:
>
> present said user with a plurality of topics;
>
> **receive a user selection of at least one topic;**
>
> **receive one or more personal details from said user associated with said at least one topic as a proposed password;**
>
> perform an Internet search using a query containing one or more keywords derived from said personal details of said proposed password, wherein said Internet search searches contents of the Internet across a plurality of web sites using a search engine tool;
>
> evaluate results of said search relative to one or more predefined thresholds applicable to said at least one selected topic;
>
> reject said proposed password when **said user is correlated with said proposed password** if one or more of said predefined thresholds are exceeded by said results; and
>
> recording said one or more personal details as a password for said user if said proposed password is not rejected.
>
> *(Emphasis Supplied)*

For the same reasons as for claim 1, the applicants respectfully traverse the rejection of claim 13.

Because claim 20 depends on claim 13, the applicants respectfully traverse the rejection of the claim 20.

Independent claim 25 recites:

> **25.** (Previously Presented) An article of manufacture for generating a password for a user during an enrollment phase, comprising a machine readable storage medium containing one or more programs which when executed implement the steps of:
>
> presenting said user with a plurality of topics;
>
> **receiving a user selection of at least one topic;**
>
> **receiving one or more personal details from said user associated with said at least one selected topic as a proposed password;**
>
> performing an Internet search using a query containing one or more keywords derived from said personal details of said proposed password, wherein said Internet search searches contents of the internet across a plurality of web sites using a search engine tool;
>
> evaluating results of said search relative to one or more predefined thresholds applicable to said at least one selected topic;
>
> rejecting said proposed password when **said user is correlated with said proposed password** if one or more of said predefined thresholds are exceeded by said results; and
>
> recording said one or more personal details as a password for said user if said proposed password is not rejected.
>
> *(Emphasis Supplied)*

For the same reasons as for claims 1 and 13, the applicants respectfully traverse the rejection of claim 25.

Ground 3: 35 U.S.C. 103 Rejection of Claims 2, 7, 11, 14, 19, and 23

Claims 2, 7, 11, 14, 19, and 23 were rejected under 35 U.S.C. 103 as being unpatentable over M. Nelson, U.S. Patent 7,062,655 (hereinafter "Nelson") in view of E. Ogura, U.S. Publication 2004/0078603 (hereinafter "Ogura") and further in view of D. Fallman, U.S. Publication 2004/0107406 (hereinafter "Fallman") and further in view of R. Eitel, U.S. Patent 7,043,521 (hereinafter "Eitel") and further in view of L. Honarvar, U.S. Patent 7,231,657 (hereinafter "Honarvar").

Because claims 2, 7, and 11 depend on claim 1, and because Honarvar fails to cure the deficiencies of Eitel, Ogura, Fallman, Nelson, Lee, and Mikheev, the applicants respectfully traverse the rejection of them.

Because claims 14, 19, and 23 depend on claim 13, the applicants respectfully traverse the rejection of them.

Ground 4: 35 U.S.C. 103 Rejection of Claims 4-6 and 16-18

Claims 4-6 and 14-16 were rejected under 35 U.S.C. 103 as being unpatentable over M. Nelson, U.S. Patent 7,062,655 (hereinafter "Nelson") in view of E. Ogura, U.S. Publication 2004/0078603 (hereinafter "Ogura") and further in view of D. Fallman, U.S. Publication 2004/0107406 (hereinafter "Fallman") and further in view of R. Eitel, U.S. Patent 7,043,521 (hereinafter "Eitel") and further in view of P-Synch Installation and Configuration Guide (hereinafter "P-Synch").

Because claims 4-6 depend on claim 1, and because P-Synch fails to cure the deficiencies of Eitel, Ogura, Fallman, Nelson, Lee, and Mikheev, the applicants respectfully traverse the rejection of them.

Because claims 16-18 depend on claim 13, and because P-Synch fails to cure the deficiencies of Eitel, Ogura, Fallman, Nelson, Lee, and Mikheev, the applicants respectfully traverse the rejection of them.

Ground 5: 35 U.S.C. 103 Rejection of Claims 9, 10, 12, 21, 22, and 24

Claims 9, 10, 12, 21, 22, and 24 were rejected under 35 U.S.C. 103 as being unpatentable over M. Nelson, U.S. Patent 7,062,655 (hereinafter "Nelson") in view of E. Ogura, U.S. Publication 2004/0078603 (hereinafter "Ogura") and further in view of D. Fallman, U.S. Publication 2004/0107406 (hereinafter "Fallman") and further in view of R. Eitel, U.S. Patent 7,043,521 (hereinafter "Eitel") and Further in view of D. Kanevsky, U.S. Patent 5,774,525 (hereinafter "Kanevsky").

Because claims 9, 10, and 12 depend on claim 1, and because Kanevsky fails to cure the deficiencies of Eitel, Ogura, Fallman, Nelson, Lee, and Mikheev, the applicants respectfully traverse the rejection of them.

Because claims 21, 22, and 24 depend on claim 13, and because Kanevsky fails to cure the deficiencies of Eitel, Ogura, Fallman, Nelson, Lee, and Mikheev, the applicants respectfully traverse the rejection of them.

CONCLUSION

The applicants have demonstrated that the logic underlying the Office's rejection is untenable, and, therefore, that the rejection is not sustainable. For this reason, the applicants respectfully request the Board of Appeals to reverse the decision of the Examiner as provided for in 37 C.F.R. 41.50(a).

Respectfully,
Amit Bagga et al.

By **/Kiril Dimov/**
Kiril Dimov
Reg. No. 60490
732-578-0103 x215

DeMont & Breyer, L.L.C.
100 Commons Way, Ste. 250
Holmdel, NJ 07733
United States of America

Claims Appendix

1. (Previously Presented) A method for generating a password for a user during an enrollment phase, comprising:

presenting said user with a plurality of topics;

receiving a user selection of at least one topic;

receiving one or more personal details from said user associated with said at least one selected topic as a proposed password;

performing an Internet search using a query containing one or more keywords derived from said personal details of said proposed password, wherein said Internet search searches contents of the Internet across a plurality of web sites using a search engine tool;

evaluating results of said search relative to one or more predefined thresholds applicable to said at least one selected topic;

rejecting said proposed password when said user is correlated with said proposed password if one or more of said predefined thresholds are exceeded by said results; and

recording said one or more personal details as a password for said user if said proposed password is not rejected.

2. (Original) The method of claim 1, further comprising the step of receiving a reminder associated with each of said one or more personal details.

3. (Canceled)

4. (Previously Presented) The method of claim 1, wherein said rejecting step employs correlation rules that are based on said at least one topic.

5. (Previously Presented) The method of claim 1, wherein said rejecting step employs one or more predefined correlation rules that ensure that answers to user selected questions cannot be qualitatively correlated with said user.

6. (Previously Presented) The method of claim 1, wherein said rejecting step employs one or more predefined correlation rules that ensure that answers to user selected questions cannot be quantitatively correlated with said user.

7. (Original)The method of claim 1, further comprising the step of sending said one or more personal details to said user as a reinforcement of said password.

8. (Original) The method of claim 1, wherein said one or more personal details are related to a personal fact from a past of said user.

9. (Original) The method of claim 1, wherein said one or more personal details are related to an experience of said user in connection with a public event.

10. (Original) The method of claim 1, wherein said one or more personal details are related to an experience of said user in connection with a private event.

11. (Original) The method of claim 1, wherein said one or more personal details can be tested during a verification phase using one or more of Boolean, multiple choice, numeric or textual queries.

12. (Original)The method of claim 1, wherein said at least one topic is selected based on psychological insights.

---

13. (Previously Presented) An apparatus for generating a password for a user during an enrollment phase, comprising:

a memory; and

at least one processor, coupled to the memory, operative to:

present said user with a plurality of topics;

receive a user selection of at least one topic;

receive one or more personal details from said user associated with said at least one topic as a proposed password;

perform an Internet search using a query containing one or more keywords derived from said personal details of said proposed password, wherein said Internet search searches contents of the Internet across a plurality of web sites using a search engine tool;

evaluate results of said search relative to one or more predefined thresholds applicable to said at least one selected topic;

reject said proposed password when said user is correlated with said proposed password if one or more of said predefined thresholds are exceeded by said results; and

recording said one or more personal details as a password for said user if said proposed password is not rejected.

14. (Original) The apparatus of claim 13, wherein said processor is further configured to receive a reminder associated with each of said one or more personal details.

15. (Canceled)

16. (Previously Presented) The apparatus of claim 13, wherein said rejecting step employs correlation rules that are based on said at least one topic.

17. (Previously Presented) The apparatus of claim 13, wherein said rejecting step employs one or more predefined correlation rules that ensure that answers to user selected questions cannot be qualitatively correlated with said user.

18. (Previously Presented) The apparatus of claim 13, wherein said rejecting step employs one or more predefined correlation rules that ensure that answers to user selected questions cannot be quantitatively correlated with said user.

19. (Original) The apparatus of claim 13, wherein said processor is further configured to send said one or more personal details to said user as a reinforcement of said password.

20. (Original) The apparatus of claim 13, wherein said one or more personal details are related to a personal fact from a past of said user.

21. (Original) The apparatus of claim 13, wherein said one or more personal details are related to an experience of said user in connection with a public event.

22. (Original) The apparatus of claim 13, wherein said one or more personal details are related to an experience of said user in connection with a private event.

23. (Original) The apparatus of claim 13, wherein said one or more personal details can be tested during a verification phase using one or more of Boolean, multiple choice, numeric or textual queries.

24. (Original) The apparatus of claim 13, wherein said at least one topic is selected based on psychological insights.

25. (Previously Presented) An article of manufacture for generating a password for a user during an enrolment phase, comprising a machine readable storage medium containing one or more programs which when executed implement the steps of:

presenting said user with a plurality of topics;

receiving a user selection of at least one topic;

receiving one or more personal details from said user associated with said at least one selected topic as a proposed password;

performing an Internet search using a query containing one or more keywords derived from said personal details of said proposed password, wherein said Internet search searches contents of the internet across a plurality of web sites using a search engine tool;

evaluating results of said search relative to one or more predefined thresholds applicable to said at least one selected topic;

rejecting said proposed password when said user is correlated with said proposed password if one or more of said predefined thresholds are exceeded by said results; and

recording said one or more personal details as a password for said user if said proposed password is not rejected.

Evidence Appendix

There is no evidence submitted pursuant to 37 CFR §§ 1.130, 1.131, or1.132.

Related Proceedings Appendix

There are no related proceedings.